CEBS 2008 156 / CEIOPS-3L3-12-08 / CESR / 08-773

16 October 2008

Common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees

Background

1. The European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees, which came into force on 1 January 2007, acts to implement the Financial Action Task Force's Special Recommendation VII in the European Union. The Regulation requires that Payment Service Providers "PSP"s (like banks and wire transfer offices) attach complete information about the payer to funds transfers made by electronic means. They must also check the information that accompanies incoming payments. The purpose of this regulation is to make it easier for the authorities to trace flows of money on occasions where that is deemed necessary.

2. This regulation sits alongside a wider body of EU and national legislation that aims to combat money laundering and the finance of terrorism, by, for example, mandating that financial institutions observe UN, EU and national sanctions, undertake due diligence checks on their customers when accounts are opened, monitor customers' behaviour on an ongoing basis, and inform the authorities when they form suspicions that they may have identified criminal or terrorist activity.

3. The Anti Money Laundering Task Force ("AMLTF") recognises that this Regulation is an important component of this wider regime. For example, when a bank checks incoming payments, it may find that information on the payer is missing or incomplete: this could be one of

the items of intelligence that contributes to a decision to file a suspicious transaction report with the authorities.

4. It has been brought to the AMLTF's attention that there appears to be an issue in relation to the information on the payer accompanying fund transfers to payment service providers of payees, arising out of this regulation. Further the Committee for the Prevention of Money Laundering and Terrorist Financing, chaired by the European Commission, and comprising of representatives from all Member States, asked the AMLTF to work on this topic, interacting with market participants. Also, the European Commission is ensuring appropriate contacts with the bodies working on payments issues too. The AMLTF has also analysed the possible conflict in the Regulation with the obligation to freeze the funds due to other provisions.

4. This paper aims to reflect a common understanding to deal with payments that lack the required information in respect of this regulation, which has been developed by the AMLTF, with the assistance of an informal consultation with the industry, including an Industry workshop held in January 2008, and has been subject to a three month public consultation launched in April 2008, which included a public hearing held on 6th May 2008.

5. This common understanding is based on the current functioning of payment, messaging and settlement systems, aims to ensure a level playing field between European payment service providers, and assist the reach of traceability[1] of transfers. This document aims to take into account the current level of compliance with the FATF Special Recommendation VII outside the EU, and the fact that funds transfers is a mass business. An annex describes some existing practices that our liaison with the financial services industry has identified. It outlines some measures that are currently being employed by payment services providers.

[1] Recital 6 of 1Directive 1781/2006 - The full traceability of transfers of funds can be a particularly important and valuable tool in the prevention, investigation and detection of money laundering or terrorist financing. It is therefore appropriate, in order to ensure the transmission of information on the payer throughout the payment chain, to provide for a system imposing the obligation on payment service providers to have transfers of funds accompanied by accurate and meaningful information on the payer.

6. The AMLTF was established in the second half of 2006 by CEBS, CESR and CEIOPS (- the three Level Three Committees, 3L3), with a view to providing a supervisory contribution in anti-money laundering (AML) and Counter Terrorism Finance issues, with a specific focus on the Third Anti-Money Laundering Directive. The AMLTF is composed of competent authorities from across Europe with supervisory responsibility for payment service providers.
7. The AMLTF acknowledges that there will be other competent authorities with these responsibilities, who are not represented on its committee. The AMLTF suggest that this paper would nonetheless represent a useful resource to these authorities.

1. Introduction

1. This paper aims to reflect the common understanding of European supervisors concerning the application of Chapter III of the European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees (hereafter referred to as the "Regulation").

2. This common understanding is based on the current functioning of payment, messaging and settlement systems and aims to ensure a level playing field between European payment service providers (hereafter referred to as PSPs). The present common understanding takes into account the current level of compliance with the Special Recommendation VII outside the EU and the fact that funds transfers is a mass business.

3. This common understanding shall not be seen as an extension to this Regulation adding obligations, but rather as a clarification on the requirements in this Regulation, so as to provide PSPs with a common understanding of supervisory expectations on compliance with this Regulation.

2. Common understanding on Article 8 of the Regulation

4. PSPs shall have effective procedures in place in order to detect whether in the messaging, payment or settlement system used to effect a transfer of funds, the fields relating to the information on the payer are complete in accordance with Articles 4 and 6. It is expected that PSPs undertake this obligation by applying both of the following elements.

5. First, as stated by the Regulation, the PSP of the payee shall detect whether, in the messaging, payment or settlement system used to effect a transfer of funds, the fields relating to the information on the payer have been completed using the characters or inputs admissible within the conventions of that messaging or payment and settlement system.

6. This first element will generally result from the mere application of the validation rules of the messaging, payment or settlement system, if those validation rules prevent payments being sent or received where the mandatory information concerning the payer is not present at all.

7. However, it is recognised that it is very difficult for a standard filter to be able to assess the completeness of all messages and that there will be instances where the payer information fields are completed with incorrect /meaningless information, where the payment will pass through the system.

8. Further PSPs are encouraged to apply filters to detect obvious meaningless information, such as information clearly intended to circumvent the intention of FATF Special Recommendation VII and this Regulation, based on their own experience, so as to assist PSPs in assessing whether they have been provided with meaningful information, as if so, the PSPs will then be obliged to reject the transfer, or to ask for information. PSPs should endeavour to apply this first element at the time of the processing.

9. Second, unless the PSP has detected the incompleteness of all transfers at the time of processing, the PSP should in addition to Article 8.1, subject incoming payment traffic to an appropriate level of monitoring to detect incomplete transfers or those with meaningless information by proceeding to appropriate post event random sampling to detect non compliant payments. Such sampling could focus more heavily on transfers from those higher risk sending PSPs, notably those PSPs who are already been identified by such sampling as having previously failed to comply with the relevant information requirement. PSPs identified as regularly failing should receive a particular attention in the application of this post event random sampling.

3. Common understanding on Articles 9 §1 and 10 of the Regulation

10. By application of Article 8 along the lines suggested above, receiving PSPs may become aware of the incompleteness/meaninglessness of the information accompanying a transfer either at the time of processing (or even before), or later if undertaking the post event monitoring.

11. The present section takes into account Article 9 §1 and Article 10. The latter particularly refers to reporting obligations set out in Chapter III of the Third Directive. Chapter III of the Third Directive notably includes Articles 22 and 24 which are particularly important for the application of Article 9§1. Those Articles are taken into account by the present guidelines. It should also be noted that Article 9 §1 of the Regulation refers to Regulations 2580/2001 and 881/2002.

3.1 The PSP becomes aware, when receiving the transfer, that it is incomplete

12. If the PSP becomes aware on receipt of the transfer, that it is incomplete, it should either reject the transfer, or ask for complete information. While it is asking for the complete information, it may either execute the transfer or hold the funds by temporarily suspending the transfer (if holding the funds is allowed by national law, bearing in mind any legal and consumer obligations).

3.1.1 Internal policy, processes and procedures

13. PSPs should adopt a policy defining their reaction on becoming aware of an incomplete transfer or with meaningless information.

14. Except for those PSPs that choose to systematically reject all such transfers, the PSP should endeavour to apply a mix of point 3.1.3, with 3.1.4 and/or 3.1.2. Without prejudice to any other applicable law or Regulation if any, the PSP should normally not execute systematically all incomplete transfers or transfers with meaningless information.

15. The PSP should define the criteria on which internal processes and procedures will be based in order to distinguish between transfers that they will execute directly and those that they will hold and/or those that they will reject. The PSP should draft those internal processes and procedures taking into account all applicable obligations. They should particularly mitigate their compliance risk when holding the funds or rejecting the transfer. Furthermore, the PSP shall particularly comply with Regulations 2580/2001 and 881/2002 and with any other lists they have an obligation to apply as it is provided by their jurisdiction.

16. The policy, processes and procedures should be approved at an appropriate hierarchic level and should be reviewed regularly.

3.1.2 The PSP chooses to reject the transfer (if allowed by national law)

17. In this case, the PSP has no obligation to ask for the complete information. When rejecting a transfer, PSPs are encouraged to give the reason for the rejection to the PSP of the payer.

18. However, the PSP shall consider the incompleteness of the transfer or meaninglessness of the information as a factor in assessing whether any transaction related to the rejected transfer is suspicious and whether it must be reported to its FIU. The assessment of suspicion should be in accordance with existing Directives and requirements.

19. Depending on the risk criteria defined by the PSP in accordance with the risk based approach, the incompleteness/meaninglessness of information may or may not trigger the necessity to assess the transaction as being suspicious. If the transaction comes from a non EEA country which EU member states consider to be equivalent to the standards of the EU Directive 2005/60/EC, this could be considered accordingly in the risk assessment. PSPs should complete this assessment in accordance with the applicable obligations and their internal processes, procedures and policies.

3.1.3 The PSP chooses to execute the transfer

20. Knowing that the transfer is incomplete or has meaningless information, the PSP chooses to execute it before asking for the complete /meaningful information to the PSP of the payer.

21. After having executed the transfer, it has to ask for complete information.

Asking the complete information

22. In this regard, the PSP should define criteria that it will use in order to determine on which occurrence it will send the request for complete information to the PSP of the payer.

23. Further, a maximum deadline between the receipt of payment and issuing a request for complete/meaningful information should be set, such as 7 working days.

24. Once the PSP has sent its request for complete/meaningful information, it should set a reasonable timeframe, such as 7 working days, or longer for messages received from outside the EEA, to receive this information and then, if the level of risk requires it, assess the suspicious character of the transaction or any related transaction and, if it did not receive a satisfactory answer to its request for further information regarding the relevant transfer, proceed to follow up on its request.

Assessing the suspicious character

25. As mentioned under point 3.1.2, PSPs should complete this assessment in accordance with the applicable obligations and their internal processes, procedures and policies. Depending on the risk criteria defined by the PSP in accordance with the risk based approach, the risk factor resulting from the incompleteness /meaninglessness of information may or may not trigger an internal transmission to the AML/CFT officer for assessment of its suspicious character.

26. In addition, it should be kept in mind that recital 16 of the Regulation particularly states that the accuracy and completeness of information on the payer should remain the responsibility of the PSP of the payer. Therefore, the PSPs of payees cannot be held responsible for the lack of information accompanying transfers they receive, including if they execute *de bona fide* a transfer without complete information on the payer that they would not have executed if the complete information had been provided.

Follow up to the request for complete information.

27. The PSP has to define policies and set up procedures and processes in order to complete an appropriate follow up to its requests for complete /meaningful information. The PSP should be able to demonstrate to its supervisor that those policies, processes and procedures are adequate in order to fulfil their objectives, and are effective in their application. The PSP could keep a record of its request, including any lack of reply, and make such a record available to the authorities.

28. For example, if the PSP of the payee did not receive a satisfactory answer to its request for complete/meaningful information after expiry of its desired timeframe, it should send a reminder, again with a desired timeframe by when it would expect to receive a response, after the first deadline has run out. The PSP may chose to batch up its follow up requests to such non responding PSPs.

29. The reminder should also notify that the sending PSP, in case it will not answer satisfactory within the deadline, will in future be subject to the internal high risk monitoring (cf. above 2.2.) and treated under the conditions of Art. 9 (2) of Regulation 1781/2006. An alternative could be that the PSP may choose to state this in its Terms and Conditions.

3.1.4 The PSP chooses to hold the funds, (if allowed by national law)

30. Section 3.1.1 of this common understanding defines how a PSP has to proceed in order to determine its reaction towards an incomplete transfer or a transfer with meaningless information. As mentioned in that section, it should be stressed that a PSP can temporarily suspend the execution of the transfer and thus holds the funds if this is requested by, or compatible with, the legal or regulatory framework to which it is subject. However, apart from suspending the transfer on the basis of the option to ask for complete information defined by Regulation 1781/2006 it may be necessary to “freeze” the funds for an undefined period of time compliant

with relevant "freezing" measures and economic sanctions (like those set out in Regulations 2580/2001 and 881/2002), with the obligation to refrain from executing transactions which are reported as suspicious (article 24(1) of Directive 2005/60/EC) and with the order to postpone such transactions issued by the competent authority (article 24(1) of Directive 2005/60/EC).Further, it is also stressed that PSPs should particularly mitigate their legal and compliance risk when holding the funds or rejecting the transfer, including in relation to their contractual obligations.

31. It can be considered that it is particularly appropriate to apply this option when there is need for clearing the situation internally or with other group members, databases or the FIU[2] in order to establish or reject the suspicion of money laundering.

32. When the PSP chooses to hold the funds, its first action should be to ask for the complete /meaningful information.

Asking for the complete information

33. In this regard, the PSP should define criteria that it will use in order to determine on which occurrence it will send the request for complete /meaningful information to the PSP of the payer. However, those processes and procedures should ensure that the PSP will ask, ideally at least once every 7 working days (or longer for payments from outside the EEA), for the complete /meaningful information from each PSP that sent at least one incomplete transfer during the previous 7 working days. The attention of the PSP is drawn on the fact that even if the maximum allowed deadline is the same as in section 3.1.3, they have to define themselves criteria in order to determine on which occurrence they will send the request. In the present section, those internally defined criteria should take into account the fact that they would in principle not be in a position to decide about rejecting the transfer or executing it as long as they will not have received the answer to the request for complete /meaningful information.

[2] FIU = Financial Intelligence Unit

34. The request for complete/meaningful information should include a deadline for the PSP of the payer to answer. A maximum deadline should be set, such as 3 working days, or longer for payments from outside the EEA. However, PSPs of payees may decide to fix a shorter deadline. This deadline could be communicated through its insertion in the Terms and Conditions of the receiving PSP.

35. Once the PSP has sent its request for complete /meaningful information, it has to wait for its selected deadline, such as 3 working days, for receiving the requested information to run out.

36. Then, if it receives a satisfactory answer to the request for complete information, it should assess the suspicious character and, after having completed this assessment, decide whether to execute the transfer, reject the transfer or sending a STR to the FIU and holding the funds.

37. The PSP has to define policies and set up procedures and processes in order to complete an appropriate follow up to its requests for complete /meaningful information. This should in particular define its reaction to the absence of a valid answer in the required deadline and the processes for sending reminders to failing PSPs. In addition, the PSP should be able to demonstrate to its supervisor that those policies, processes and procedures are adequate in order to fulfil their objectives and are effectively applied.

38. For example, if it does not receive a satisfactory answer to the request for complete /meaningful information, it should proceed to the follow up to the request. This follow up could consist of sending a reminder, such as 3 working days after the first deadline has run out. The reminder should set a deadline for the sending PSP, which could be again 3 working days. The reminder could also notify that the sending PSP, in case it will not answer satisfactory within the deadline, will in future be subject to the internal high risk monitoring (cf. above 2.2.) and treated under the conditions of

Art. 9 (2) of Regulation 1781/2006. Another alternative could be that the PSP may choose to state this in its Terms and Conditions.

39. Additionally, the reminder should indicate that the respective transfer is currently pending. After that the deadline included in the reminder has run out, and whether or not it has received a satisfactory answer to its reminder, the receiving PSP should assess the suspicious character and, after having completed this assessment, decide whether to execute the transfer, reject the transfer or send a STR to the FIU and hold the funds. When it decides to execute the transfer, it has to take into account the factors that led him to hold the funds at the initial stage. For more details on *"Assessing the suspicious character",* refer to section 3.1.3.

3.2 The PSP becomes aware that a transfer is incomplete after having executed the transfer

40. Where the PSP of the payee becomes aware subsequent to processing the payment that it contained meaningless or incomplete information either as a result of random checking or by any other way, it must:
    a. consider the incompleteness /meaninglessness of the information as a factor in assessing whether the transfer or any related transaction is suspicious and whether it must be reported to its FIU;
    b. consider asking for the complete /meaningful information to the PSP of the payer or, where appropriate, to the intermediary PSP. In this case, it shall also proceed to the follow up actions to the request, as above mentioned.

4. Common understanding on Article 9 §2

4.1 The regularity of failure

41. Recital 17 calls for a common approach on Article 9 §2, which provides that PSPs have to react towards PSPs that are regularly failing to supply the complete information.

42. However, the Regulation does not elaborate on the concept of regularity. A common approach on this point will be highly desirable as a common response by EU PSPs will enhance the credibility and effectiveness of their reaction and, thereby, international compliance with FATF Special Recommendation VII, SR VII. The PSP of the payee shall determine when the other PSP is regularly failing. This could be due to different reasons, for example regularly not inserting the full information of the payer and/or regularly not responding to requests in a timely manner. Also the level of failure may vary according to the risk based approach of the payee PSP.

43. Accordingly the PSP of the payee shall consider what criteria determine whether the PSP of the payer has regularly failed to provide the required information. Until the PSP of the payee, has sufficient data to analyse its own experience in identifying such 'failure", the following criteria could, for example, be used:

a. the level of cooperation of the PSP of the payer relating to requests for complete/meaningful information sent ;
b. a threshold defined in a percentage of incomplete transfers or transfers with meaningless information sent by a specific PSP;
c. a threshold defined in a percentage of still incomplete transfers in a period or with meaningless information, after that the PSP of the payer has received a certain amount of requests for complete/meaningful information;

d. a threshold defined equating to an absolute number of incomplete transfers or transfers with meaningless information sent by a specific PSP; and
e. a threshold defined equating to an absolute number of still incomplete transfers or transfers with meaningless information in a defined period, after that the PSP of the payer has received a certain amount of requests for complete/meaningful information.

4.2 Steps to be taken

44. Once a PSP has been assessed as regularly failing by a PSP of a payee, the PSP of the payee should issue a warning to the PSP which is failing, in order to draw its attention to the fact that, in accordance with the present common understanding, it has been identified as regularly failing.

4.3 Transmission to the authorities

45. As provided by Article 9§2, once a PSP has been identified as being regularly failing to provide the required information, the PSP of the payee shall report that fact to the "authorities responsible for combating money laundering or terrorist financing". Determination of such "authorities responsible" remains within national arrangements, and they should receive this information. These "authorities" are encouraged to exchange the information with their national supervisors.

46. This transmission of such information should be clearly distinguished from a Suspicious Transaction Report, STR. Indeed, the purpose of this transmission is to signal that a specific PSP meets the criteria defining the regular failure in this common understanding, which indicates a difficulty to comply with SR VII. This transmission does not imply that the PSP of the payer is suspected of money laundering or terrorism financing. It implies that it might be failing to respect its obligations under SR VII. Some countries have chosen to develop a specific format for "Article 9 §2

reporting". This seems to enhance the perception of this distinction by PSPs.

4.4 Decision as to restrict or terminate the business relationship with a PSP reported as being regularly failing

47. The Regulation states that the PSP of the payee decides whether or not to restrict or terminate its business relationship with regularly failing PSPs.

48. For the PSP of the payee to act alone against a failing PSP may prove commercially disruptive, particularly where that PSP is an important counterparty.

49. In addition, we would also expect supervisors to share views about failing PSPs and consider what action they may take.

50. It should be stressed that, when the regularly failing PSP is also a correspondent bank from a third country, the decision taken according to the present section and the enhanced due diligence performed according to Article 13 §3 of the Third Anti Money Laundering Directive could all be included as part of the process of managing the cross-border correspondent bank's relationship.

5. Internal data collecting and reporting

51. PSPs should be able to demonstrate to their supervisory authority that there are effective policies and procedures in place related to data collection and internal reporting that are appropriate to meeting the requirements of the Regulation. Further, PSPs' internal control and audit policies and procedures for Anti Money Laundering and Combat of Financing of Terrorism should be subject to appropriate senior management oversight.

6. Threshold

52. It should be born in mind, when applying the Regulation and the present common understanding, that some countries outside the EU may have framed their own Regulation to incorporate a threshold of €/US$ 1,000 below which the provision of complete information on out-going payments is not required. This is permitted by the Interpretative Note to SR VII. This does not preclude European PSPs from calling for the complete information where it has not been provided. The existence of such a threshold, although relevant for the risk-based decision whether to carry out, to hold or to reject the transaction as well as for the determination of the regularity of failures, does not exclude the application of the procedures under points 3 and 4 above.

53. Any threshold of a higher amount would be non compliant with the SR VII and any related transfer will have to be considered as incomplete.

7. Review of the common understanding

54. Considering the fact that the common understanding takes into account the current level of compliance with SR VII at international level and the current functioning of payment, settlement, and supporting systems, it should be revised subject to the compliance level attained by the Industry with the regulations, and not later than when the Regulation 1781/2006 is reviewed.

Annex 1

Existing industry practice

This annex describes some existing practice that our liaison with the financial services industry has identified. It outlines some measures that are currently being employed by payment service providers.

- Bank N is a large bank based in an EU member state. It handles tens of thousands of electronic transfers every day. It sends and receives payments between EU member states, and countries outside of the EU, using the SWIFT message system. The SWIFT system prevents messages with blank fields from being processed. However, meaningless data can still be attached to payments: the SWIFT messaging systems are not able to prevent this. As such, Bank N undertakes post-event sampling of incoming payments traffic to identify where data is likely to be incomplete or meaningless. Sampling is focused on certain areas that are regarded to present a higher risk. Examples of higher-risk payments identified by Bank N include a) those that originate from payment service providers outside the EU, particularly those from jurisdictions that the bank has identified to be of a higher risk b) those from payment service providers that have previously failed to meet their obligations and c) payments that are collected by the payee in cash on a "pay on application and identification basis".

- Bank P is a small private bank based in a European capital that predominantly deals with customers from certain countries outside the EU. It receives very few electronic payments on behalf of its customers. When these payments are received it is not unusual for these to have originated from outside the EU, and to represent large sums of money. Bank P is able to subject each payment to scrutiny by a member of staff. The staff member's knowledge of the countries in question allows

them to quickly identify where, for example, the payer's address appear to not correspond with what might be expected.

- Bank Q is a medium-sized bank in an EU state. Bank Q seeks to identify incorrect data by performing post-event sample checks. As such, the payment has already been made by the time that Bank Q has become aware that information is incorrect. Aside from the practical issues, Bank Q is unsure whether it would be desirable to reject a transaction "in-flight": this could lead to civil claims for breach of contract, and also risk prosecution under national legislation that outlaws "tipping off" criminals. The next step that the bank takes is to seek complete information on the payer. It also considers whether there is anything suspicious about the transaction, although it is difficult to form suspicions based on this information alone. Bank Q is recording where payment service providers are failing to provide information, and considering which institutions are being sufficiently unreliable or unco-operative to warrant further action. Bank Q has not ruled out ending relationships with some payment service providers outside of the EU.

- For intermediaries, many view that the Payee PSP should address a request for missing information direct to the Payer PSP. It should not be necessary to involve the intermediary PSP, other than on occasions where their help is needed to provide a payer PSP transaction reference number in order to trace the payment.

- Some banks view that is sufficient to have information in Field 20 in the Swift standard message and that this meets the obligation according to the Regulation for a “unique identifier”. However, in non EU payments there must be information on the banks account in Field 50 in the Swift message.

Annex 2

Summary of Industry workshop on Anti Money Laundering in relation to the European regulation on the information on the payer accompanying funds transfers

London, 9th January 2008

1. A workshop was held with industry participants and the Anti Money Laundering Task Force ("AMLTF") on obligations imposed by the EU Regulation 1781/2006, implemented in December 2007. The AMLTF Chair, Andrea Enria, Secretary General of CEBS, provided background on the AMLTF, which was established in the second half of 2006 by CEBS, CESR and CEIOPS (- the three Level Three committees, 3L3), with a view to providing a supervisory contribution in anti-money laundering (AML) and Counter Terrorism Finance issues, with a specific focus on the Third Anti-Money Laundering Directive. In particular, its mandate is focused on the developments of risk-based approaches to Customer Due Diligence (CDD) and the "know your customer principle" (KYC) and their impact on the internal organisation and controls of intermediaries. The AMLTF provides a forum for exchange of experiences and networking between supervisory authorities, to help identifying practical issues that supervisors face in their day-to-day work and, when possible find common practical answers.
2. The workshop had been convened as the AMLTF wishes to find practical solutions to deal with payments that lack the required information in respect of the Regulation 1781/2006.
3. Further the Committee for the Prevention of Money Laundering and Terrorist Financing (CPMLTF), chaired by the European Commission and comprises of representatives from all Member States, asked the AMLTF to work on this topic, interacting with market participants. Also, the Commission is ensuring appropriate contacts with the bodies working on payments issues too.
4. The CBFA AMLTF member presented the AMLTF's (draft) paper AMLTF 2007 22 rev2, relating to information on the payer of accompanying

fund transfers to payment service providers of payees, and sought to gather industry views on the nature and relevance of the problem, to assist in AMLTF finalising this paper and discussing the issues at the CPLMTF. In particular the CBFA AMLTF member presented issues relating to the general principles for common understanding on Articles 8, 9, 10 and 16 of Reg. 1781/2006. In adherence to standard 3L3 practices for public consultation, the AMLTF intends to finalise this paper, and subject it to formal consultation, and hence workshop attendees' comments were sought informally on the current draft.

5. Discussion focussed on incomplete incoming transactions messages, both inter EEA and from 3rd countries. Market participants agreed that the problem is indeed relevant and expressed their availability to provide information on the amount and distribution (including, in terms of country of origin and Payment Service Providers) of the transactions with incomplete information.
6. The industry representatives also presented their approaches to dealing with the issue. Some differences emerged both in the timing of the assessment of the completeness of information as per Art 9.1 and in the interpretation of Art 9.2. An issue relating to Art 6 was also raised, calling for further investigation: it was pointed out that a reference number might be sufficient for funds transfer inter EEA, yet from a practical perspective, might not be sufficient for many competent authorities, in relation to their domestic AML/financial crime requirements.
7. Some concerns were expressed as to the compliance burden of some of the options presented in the draft AMLTF paper (i.e. under Art 9.1 and Art 10) where the AMLTF proposed i) PSP execute the transfer first and then ask for complete information. PSP wait for deadline for receiving the complete information to run out and then assess the suspicious character of the transaction; and ii) PSP define risk criteria in order to allow their systems to distinguish between those incomplete transfers that can be executed before assessing their suspicious character and those incomplete transfers for which the assessment of their suspicious character and the request for complete information should be done

before executing the transfer. Some also suggested that there may be an additional option, or that a mix of options should be sought that better reflects current market practices.

8. Although the urgency of the subject matter was acknowledged, several market participants invited the AMLTF not to rush to conclusions, especially in some areas.
9. The AMLTF Chair committed to come back to the industry group with:
    a. a request for some information by early February, and
    b. to submit, for an informal feedback, a revised version of the paper as soon as available; and
10. Further in adherence to standard 3L3 practices for public consultation, the AMLTF aims to subject its proposals for a 3 month public consultation, relatively soon, although there may be more flexibility in the consultation period so as to respect the urgency of finding a solution to the problem, having taken into account the informal pre consultation with industry.